

Notice of Allowability

Application No. **10/803,263**

Applicant(s) **OZLUTURK, FATIH M.**

Examiner **Jean B Corielus**

Art Unit **2637**

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 1/28/05&5/2/05.
2. ☒ The allowed claim(s) is/are 1-8.
3. ☒ The drawings filed on 18 March 2004 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|--|
| <ol style="list-style-type: none">1. <input type="checkbox"/> Notice of References Cited (PTO-892)2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | <ol style="list-style-type: none">5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)6. <input checked="" type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance9. <input type="checkbox"/> Other _____ |
|--|--|


Jean B Corielus
Primary Examiner
Art Unit: 2637

5-14-05

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jeffrey Glabicki on 4/25/05.

IN THE CLAIMS:

1. (currently amended) A circuit for generating a cipher stream, the circuit comprising:

a first and a second plurality of linear feedback shift registers (LFSR), each LFSR of the first of the second plurality of LFSR having an initial value of not all zero bits;

a first of the second plurality of LFSR having a clock signal as a clock input and others of the second plurality of LFSR each having an output of a previous one of the second plurality of LFSR as a clock input;

a first of the first plurality of LFSR having the clock signal combined with an output of the first of the second plurality of LFSR as a clock input and others of the first plurality of LFSR each having an output of a corresponding [previous] one of the others of the second plurality of LSFR combined with an output of a previous one of the first plurality of LFSR as a clock input; and

an output of a last of the first plurality of LFSR and an output of a last of the second plurality of LFSR being combined to produce the cipher stream.

3. (currently amended) The circuit of claim 1 wherein the combining of the output of a corresponding [previous] one of the others of the second plurality of LSFR with an output of a previous one of the first plurality of LSFR is performed by an AND gate.

5. (currently amended) A software [Software] configured to produce a cipher stream, the software effectively modeling a circuit having components comprising:

a first and a second plurality of linear feedback shift registers (LFSR), each LFSR of the first of the second plurality of LFSR having an initial value of not all zero bits;

a first of the second plurality of LFSR having a clock signal as a clock input and others of the second plurality of LFSR each having an output of a previous one of the second plurality of LFSR as a clock input;

a first of the first plurality of LFSR having the clock signal combined with an output of the first of the second plurality of LFSR as a clock input and others of the first plurality of LFSR each having an output of [one] a corresponding [previous] one of the others of the second plurality of LSFR combined with an output of a previous one of the first plurality of LFSR as a clock input; and

an output of a last of the first plurality of LFSR and an output of a last of the second plurality of LFSR being combined to produce the cipher stream.

7. (currently amended) The software of claim 5 wherein the combining of the output of a corresponding [previous] one of the others of the second [first] plurality of LSFR with an output of a previous one [another of another] of the first plurality of LSFR is performed by an AND gate.


The following is an examiner's statement of reasons for allowance: an apparatus for generating a cipher stream is disclosed. The closest prior art, Dent, US Patent No. 5,148,485, Kencheng Zeng et al, "pseudo random bit generators in stream-cipher cryptography computer, vol. 24, No.2, 2/1/91, page 8-17, discloses the invention substantially as claimed but do not explicitly teach the limitations of "a first of the first plurality of LFSR having the clock signal combined with an output of the first of the second plurality of LFSR as a clock input and others of the first plurality of LFSR each having an output of [one] a corresponding [previous] one of the others of the second plurality of LSFR combined with an output of a previous one of the first plurality of LFSR as a clock input". Such limitations, as recited in claims 1 and 5, are neither anticipated nor rendered obvious by the Dent and the Kencheng Zeng et al references taken alone or in combination.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jean B Corrielus whose telephone number is 571-272-3020. The examiner can normally be reached on Maxi-Flex.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jay Patel can be reached on 571-272-3086. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Jean B Corrielus
Primary Examiner
Art Unit 2637 5.14.05